

1 AI LAW, PLC
2 Ahmed Ibrahim, State Bar No. 238739
3 4343 Von Karman Ave, Suite 250
4 Newport Beach, CA 92660
5 Ph.: 949-260-1240
6 Fax: 949-260-1280
7 aibrahim@ailawfirm.com

8 Attorneys for Plaintiff, Individually and On
9 Behalf of All Others Similarly Situated

10
11 **UNITED STATES DISTRICT COURT**
12 **CENTRAL DISTRICT OF CALIFORNIA**
13

14 ARIFUR RAHMAN, an individual, on
15 behalf of himself and all others similarly
16 situated,

17 Plaintiff,

18 vs.

19 MARRIOTT INTERNATIONAL, INC., a
20 Delaware Corporation, DOES 1-100,
21 inclusive,

22 Defendants.
23

CASE NO.: 8:20-cv-00654

CLASS ACTION COMPLAINT FOR:

(1) NEGLIGENCE

**(2) VIOLATION OF THE
CALIFORNIA CONSUMER
PRIVACY ACT (Cal. Civ. Code §
1798.150)**

(3) BREACH OF CONTRACT

**(4) BREACH OF IMPLIED
CONTRACT**

(5) UNJUST ENRICHMENT

**(6) VIOLATION OF THE
CALIFORNIA UNFAIR
COMPETITION LAW (CAL. BUS.
& PROF. CODE § 17200, et seq.)**

DEMAND FOR JURY TRIAL

1 Plaintiff Arifur Rahman (“Plaintiff”), on behalf of himself and all others similarly
2 situated, hereby alleges as follows:

3
4 **I. BACKGROUND**

5 1. This action arises out of a massive cybersecurity breach affecting 5.2 million
6 consumers who entrusted their highly sensitive personal and confidential information to
7 defendant Marriott International, Inc. (“Marriott”). Marriott announced the data breach on
8 March 31, 2020 and sent e-mails to customers affected by the security debacle, informing
9 them that information such as names, addresses, phone numbers, and e-mail addresses—
10 all information that is solid gold for identity thieves—were accessed by unauthorized
11 persons. This catastrophic and inexcusable mishap was unmistakably the result of
12 Marriott’s complete failure to exercise reasonable care and implement adequate security
13 systems, institute the most basic cybersecurity policies and procedures, and adequately
14 train employees and franchisees on such policies and procedures. In this action, Plaintiff,
15 on behalf of a class of similarly situated California residents, seeks to hold Marriott
16 accountable for its utter disregard for the privacy and sanctity of its customer’s data—data
17 that Marriott does not hesitate to take from customers for marketing analytics to upsell and
18 increase revenues and to even share with third-parties, while making \$20 Billion in
19 revenue. Fortunately for consumers, the legislature passed the California Consumer
20 Privacy Act (Cal. Civ. Code § 1791.100, *et seq.*) so that companies may finally learn their
21 lesson when it comes to securing consumer data and being honest with them about what
22 they are doing with that data. Indeed, it is no coincidence that the Act confers on private
23 citizens the ability to bring civil actions for the failures of companies like Marriott to protect
24 sensitive consumer data from a breach like the one at issue here. Plaintiff and the class
25 members intend to vindicate those rights in this case.

26
27 **II. PARTIES**

28 2. Plaintiff Arifur Rahman (“Plaintiff”) is an individual who is a citizen of the

1 State of California and resident of the County of Orange.

2 3. Defendant Marriott International, Inc. (“Marriott” or “Defendant”) is a
3 Delaware corporation with its principal place of business in Bethesda, Maryland.

4 4. The true names and capacities of defendants DOES 1 through 100, inclusive,
5 whether individual, plural, corporate, partnership, associate or otherwise, are not known to
6 Plaintiff, who therefore sues said defendants by such fictitious names. Plaintiff is informed
7 and believes and thereon alleges that each of the defendants designated herein as DOE is
8 in some manner responsible for the acts and occurrences set forth herein. Plaintiff will
9 seek leave of court to amend this Complaint to show the true names and capacities of
10 defendants DOES 1 through 100, inclusive, as well as the manner in which each DOE
11 defendant is responsible, when the same have been ascertained.

12 5. Plaintiff is informed and believes, and upon such basis alleges, that at all times
13 herein mentioned, each of the defendants herein was an agent, servant, employee, co-
14 conspirator, partner, joint venturer, wholly owned and controlled subsidiary and/or alter
15 ego of each of the remaining defendants, and was at all times acting within the course and
16 scope of said agency, service, employment, conspiracy, partnership and/or joint venture.

17 6. Defendants, and each of them, aided and abetted, encouraged and rendered
18 substantial assistance in accomplishing the wrongful conduct and their wrongful goals and
19 other wrongdoing complained of herein. In taking action, as particularized herein, to aid
20 and abet and substantially assist the commission of these wrongful acts and other
21 wrongdoings complained of, each of the defendants acted with an awareness of its primary
22 wrongdoing and realized that its conduct would substantially assist the accomplishment of
23 the wrongful conduct, wrongful goals, and wrongdoing.

24
25 **III. JURISDICTION AND VENUE**

26 7. This Court has subject matter jurisdiction over this action pursuant to the Class
27 Action Fairness Act of 2005 and 28 U.S.C. section 1332 because the total matter in
28 controversy exceeds \$5 Million and there are over 100 members of the proposed class.

1 Further, at least one member of the proposed class is a citizen of a State different from at
2 least one defendant.

3 8. Venue is proper pursuant to 28 U.S.C. section 1391(b)(2) because a
4 substantial part of the events or omissions giving rise to the claim occurred in this judicial
5 district. Venue is also proper pursuant to 28 U.S.C. section 1391(b)(1) and (c)(2) because
6 Defendant Marriott is subject to the Court's personal jurisdiction in this judicial district.

7 8 **IV. GENERAL ALLEGATIONS**

9 **A. Company Background.**

10 9. Marriott International is a multinational, diversified hospitality company that
11 manages and franchises a broad portfolio of hotels and related lodging facilities, including
12 30 brands with more than 7,000 properties across 130 countries and territories globally.
13 Marriott has a broad presence throughout California, where there are numerous Marriott
14 properties. Founded in 1927, the company is headquartered in Bethesda, Maryland, and
15 maintains hotel brands including Marriott, Courtyard, and Ritz-Carlton. Marriott reported
16 revenues of \$20.97 billion in the 2019 fiscal year.

17 10. Guests make reservations to stay at Marriott hotels in multiple ways, including
18 through Marriott's website, <http://www.marriott.com>. When making a reservation,
19 Marriott requires guests to provide certain personal information including name, address,
20 email address, phone number, and payment card information. In some instances, Marriott
21 also collects passport information, room preferences, travel destinations, and other personal
22 information. Similarly, when creating an account to become a member of Marriott's
23 customer loyalty program ("Marriott Bonvoy"), guests provide much of the same
24 information specified above, as well as additional personal information such as date of birth
25 and loyalty numbers of Marriott partners (e.g., airlines). Collectively, this information
26 shall be referred to hereafter as "Personal Information." This Personal Information resides
27 on databases maintained by Marriott and from which Marriott derives numerous benefits,
28 including the ability to analyze the data to enhance their abilities to upsell and market hotels

1 and resorts to their guests, as well as in some cases, obtain direct monetary benefits for
2 sharing data with third parties.

3 11. Personal Information provided by customers is governed by Marriott’s Global
4 Privacy Statement, which provides detailed information about what types of Personal
5 Information will be shared, with what entities, and how it is collected. In its Global Privacy
6 Statement dated June 3, 2019, Marriott assures customers that “[t]he Marriott Group, which
7 includes Marriott International, Inc. . . . values you as our guest and recognizes that privacy
8 is important to you.” It states that the Marriott Group collects data:

9 (a) through websites operated by us from which you are accessing this
10 Privacy Statement, including Marriott.com and other websites owned or controlled by the
11 Marriott Group.

12 (b) through the software applications made available by us for use on or
13 through computers and mobile devices.

14 (c) through our social media pages that we control from which you are
15 accessing this Privacy Statement

16 (d) through HTML-formatted email messages that we send you that link to
17 this Privacy Statement and through your communications with us when you visit or stay as
18 a guest at one of our properties, or at homes and villas offered on the Homes and Villas by
19 Marriott International platform, or through other offline interactions.

20 12. In a section of the Global Privacy Statement entitled “Collection of Personal
21 Data,” Marriott Group communicates to customers that “[a]t touchpoints throughout your
22 guest journey, we collect Personal Data in accordance with law[.]” Marriott Group defines
23 “Personal Data” as “data that identify you as an individual or relate to an identifiable
24 individual.” This includes, according to Marriott Group:

- 25 • Name
- 26 • Gender
- 27 • Postal address
- 28 • Telephone number

- 1 • Email address
- 2 • Credit and debit card number or other payment data
- 3 • Financial information in limited circumstances
- 4 • Language preference
- 5 • Date and place of birth
- 6 • Nationality, passport, visa or other government-issued identification
- 7 data
- 8 • Important dates, such as birthdays, anniversaries and special occasions
- 9 • Membership or loyalty program data (including co-branded payment
- 10 cards, travel partner program affiliations)
- 11 • Employer details
- 12 • Travel itinerary, tour group or activity data
- 13 • Prior guest stays or interactions, goods and services purchased, special
- 14 service and amenity requests
- 15 • Geolocation information
- 16 • Social media account ID, profile photo and other data publicly
- 17 available, or data made available by linking your social media and
- 18 loyalty accounts

18 13. “In more limited circumstances,” Marriott Group communicates to customers
19 that it may also collect:

- 20 • Data about family members and companions, such as names and ages
- 21 of children
- 22 • Biometric data, such as digital images
- 23 • Images and video and audio data via: (a) security cameras located in
- 24 public areas, such as hallways and lobbies, in our properties; and (b)
- 25 body-worn cameras carried by our loss prevention officers and other
- 26 security personnel
- 27 • Guest preferences, enquiries and comments and any other personalized
- 28 data, such as your interests, activities, hobbies, food and beverage
- choices, services and amenities of which you advise us or which we
- learn about during your visit

1 14. This data is collected in a variety of ways, according to Marriott Group,
2 including through online services, property visits and offline interactions, customer care
3 centers, owners and franchisees, homes and villas property management companies,
4 authorized licensees, strategic business partners, joint marketing partners, Internet-
5 connected devices, and physical and mobile location-based services.

6 15. In a section of the Global Privacy Statement entitled “Security,” Marriott
7 Group claims that “[w]e seek to use reasonable organizational, technical and administrative
8 measures to protect Personal Data.”

9 16. In addition to this Global Privacy Statement, Marriott published on January 1,
10 2020 a statement specific to California residents on its website, entitled the “California
11 Consumer Privacy Statement.” In it, Marriott Group purports to provide what it refers to
12 as “additional details” concerning the “the categories of Personal Information about
13 California residents that we have collected or disclosed within the preceding 12 months[.]”
14 It states that it collects the “following categories of Personal Information” from California
15 residents:

16 (a) Identifiers, such as name, nationality, passport, visa or other
17 government-issued identification data, and online identifiers;

18 (b) Personal information, as defined in the California safeguards law, such
19 as name, contact information, and financial information;

20 (c) Characteristics of protected classifications under California or federal
21 law, such as gender, age, medical conditions, primary language, national origin,
citizenship, and marital status;

22 (d) Commercial information, such as transaction information, purchase
23 history, financial details, payment methods, and membership or loyalty program data.

24 17. Marriott Group further states that in more limited circumstances, it may also
25 collect the following categories of “Personal Information”:

26 (a) Internet or network activity information, such as browsing history and
interactions with our and other websites and computer systems;

27 (b) Geolocation data, such as device location and IP location;

28 (c) Audio, electronic, visual and similar information, such as images and

1 audio, video or call recordings created in connection with our business activities;

2 (d) Inferences drawn from any of the Personal Information listed above to
3 create a profile or summary about, for example, an individual's preferences and
4 characteristics.

5 18. Marriott recognizes the value of this personal information of customers as
6 evidenced by the fact that Marriott employs a customer analytics company for the
7 systematic examination of its customer information to identify, attract, and retain the most
8 profitable customers and to predict future behaviors. According to Marriott, "there is no
9 lack of available data: household profile, including number of kids; type of jobs held by
10 family members; their salaries; where and how they spend their money and even the type
11 of jeans they buy." D. Eisen, *Marriott Bets on Predictive Analytics for Brand Growth*,
12 QUESTEX LLC (Jan. 31, 2018), [https://www.hotelmanagement.net/tech/marriott-builds-its-](https://www.hotelmanagement.net/tech/marriott-builds-its-brands-by-knowing-more-about-you)
[brands-by-knowing-more-about-you](https://www.hotelmanagement.net/tech/marriott-builds-its-brands-by-knowing-more-about-you)

13 19. Plaintiff and the class members provided their Personal Information to
14 Marriott with the expectation and understanding that Marriott would adequately protect
15 and store their data. If they had known that Marriott's data security was insufficient to
16 protect their Personal Information, they would not have entrusted their Personal
17 Information to Marriott and would not have been willing to pay for, or pay as much for,
18 hotel reservations at Marriott properties and other amenities. Despite collecting the
19 Personal Information of millions of consumers worldwide and, more specifically, of
20 California consumers, Marriott failed to prioritize data security by adopting reasonable data
21 security measures to prevent and detect unauthorized access to their highly-sensitive
22 databases. Marriott had the resources to prevent a breach and made significant
23 expenditures to market their hotels and hospitality services, but neglected to adequately
24 invest in data security, despite the growing number of well-publicized data breaches
25 affecting the hospitality and similar industries.

26 **B. The Data Breach.**

27 20. On March 31, 2020, Marriott announced a data breach affecting **5.2 million**
28 customers in a statement posted on its website entitled "Marriott International: Incident

1 Notification.” In the posting, Marriott stated that at the end of February 2020, Marriott
2 “identified that an unexpected amount of guest information may have been accessed using
3 the login credentials of two employees at a franchise property.” According to Marriott,
4 “[w]e believe this activity started in mid-January 2020.” Marriott claimed that upon
5 discovery, it confirmed that the login credentials were disabled and it began an
6 investigation—an investigation that Marriott admits is “ongoing” and thus has not been
7 completed.

8 21. Marriott admits that “[a]t this point, we believe that the following information
9 may have been involved,” claiming that not all of the information was present for every
10 guest involved:

- 11 • Contact details (e.g., name, mailing address, email address, and phone
12 number)
- 13 • Loyalty Account Information (e.g., account number and points balance)
- 14 • Additional Personal Details (e.g., company, gender, and birthday day
15 and month)
- 16 • Partnerships and Affiliations (e.g., linked airline loyalty programs and
17 numbers)
- 18 • Preferences (e.g., stay/room preferences and language preference)

19 22. In answering the question “How many guests were involved in this incident?”
20 Marriott states “Although Marriott’s investigation is ongoing, the company currently
21 believes that information may have been involved for up to approximately 5.2 million
22 guests.”

23 23. Although Marriott contends in the statement that it “currently has no reason
24 to believe” that other information was breached, it does not and cannot say so definitively
25 and, as noted above, advised customers that its investigation is “ongoing.”

26 24. Marriott also directed customers to a “self-service online portal” that it set up
27 to enable guests “to determine whether their information was involved in the incident and,
28 if so, what categories of information were involved.” The portal was made accessible to
customers via a hyperlink that redirected guests to a purportedly secure site where

1 customers could enter their name, e-mail address, country or region, and their customer
2 loyalty program number (optional) to obtain more information about whether they were a
3 victim of the data breach.

4 **C. Plaintiff Is A Confirmed Victim of the Data Breach.**

5 25. Plaintiff is a Marriott Bonvoy member and has spent money on many
6 occasions to stay at Marriott properties. In connection with his Marriott Bonvoy account,
7 along with making guest reservations to stay at Marriott properties and making purchases
8 from said properties, Plaintiff has entrusted a litany of Personal Information to Marriott,
9 and Marriott has collected and stored such information from Plaintiff, including, without
10 limitation, his name, address, e-mail address, phone number, date of birth, and payment
11 information.

12 26. On March 31, 2020, Plaintiff and other affected customers, including the
13 members of the class, received a signed e-mail from Stephanie C. Linnartz, Marriott's
14 Group President, Consumer Operations, Technology and Emerging Businesses. In the e-
15 mail, Ms. Linnartz notified Plaintiff and other customers of the data security breach and
16 advised them that their personal information may have been compromised. She stated:
17 "We are writing to let you know that some of your information may have been accessed
18 without authorization. We are sorry that this occurred, and this message explains what
19 happened, how we can assist you, and steps you can take."

20 27. The remainder of the e-mail was similar to the announcement described above
21 that was posted on Marriott's website the same day with one important and notable
22 exception. Unlike the website posting, the e-mail sent to customers did *not* advise them
23 that they could access a "self-service portal" where they would be able to determine
24 whether their information was accessed in the breach. Rather, in what was obviously a
25 cheap ploy to make it more unlikely that customers would find out whether their data had
26 been stolen, Marriott put its customers through their paces. They made them first read the
27 initial e-mail, then find the link to the announcement at <http://mysupport.marriott.com>, then
28 re-read the announcement (which on its face appeared identical to the e-mail), find the

1 sentence relating to the portal (if they noticed it at all), click on the portal link, enter the
 2 information requested, receive a notification e-mail from the portal, and then return back
 3 to the portal to view the message.

4 28. After visiting the portal and entering the information requested, Plaintiff
 5 received a notification to his e-mail address prompting him to return to the portal to open
 6 a message he received. Shortly thereafter, Plaintiff received in the portal a message from
 7 the “Privacy Team” at the “Marriott Privacy Center” confirming that his personal data had,
 8 in fact, been involved in the data security breach. The message to Plaintiff states, in
 9 relevant part (with emphasis added), the following:

10 We are in receipt of your inquiry regarding whether your
 11 personal data was involved in the property system incident that
 12 was announced in March 2020 (the Incident).

13 Based on the email address and/or Marriott Bonvoy number that
 14 you provided to us, **we believe that your information was
 15 involved.** Following our analysis, **we currently believe that the
 16 following categories of information about you were involved
 17 in the Incident**

18 **Contact details (e.g., name, mailing address, email address,
 19 and phone number),** Additional personal details (e.g.,
 20 company, **gender, and birthday day and month**), Loyalty
 21 account information (e.g., **account number** and points balance,
 22 but not passwords), Partnerships and affiliations (e.g., **linked
 23 airline loyalty programs and numbers**), Preferences (e.g.,
 24 stay/room preferences and language preference)

25 29. The fact that Plaintiff’s and class members’ Personal Information was
 26 accessed without authorization establishes that Marriott did not take adequate data security
 27 measures to store and protect its guests’ Personal Information. Marriott failed to take
 28 adequate security measures to protect Plaintiff’s and the class members’ Personal
 Information.

26 **D. The Effects of the Data Breach on Victims of Marriott’s Data Breach.**

27 30. Marriott’s failure to keep Plaintiff’s and class members’ Personal Information
 28 secure has severe ramifications. Given the sensitive nature of the Personal Information

1 stolen in the Marriott data security breach at issue, including names, addresses, phone
2 numbers, e-mail addresses, dates of birth, and account numbers—hackers have the ability
3 to commit identity theft and other identity-related fraud against Plaintiff and class members
4 now and into the indefinite future.

5 31. The Personal Information exposed is highly coveted and valuable on
6 underground or black markets. For example, a cyber “black market” exists in which
7 criminals openly post and sell stolen consumer information on underground Internet
8 websites known as the “dark web”—exposing consumers to identity theft and fraud for
9 years to come.

10 32. Personal Information of the type breached in this case has significant
11 monetary value in part because criminals continue their efforts to obtain this data. *Data*
12 *Breaches Rise as Cybercriminals Continue to Outwit IT*, CIO MAGAZINE, Sept. 28, 2014,
13 available at [http://www.cio.com/article/2686167/data-breach/data-breaches-rise-as-](http://www.cio.com/article/2686167/data-breach/data-breaches-rise-as-cybercriminals-continue-to-outwit-it.html)
14 [cybercriminals-continue-to-outwit-it.html](http://www.cio.com/article/2686167/data-breach/data-breaches-rise-as-cybercriminals-continue-to-outwit-it.html). In other words, if any additional breach of
15 sensitive data did not have incremental value to criminals, one would expect to see a
16 reduction in criminal efforts to obtain such additional data over time. Instead, just the
17 opposite has occurred. For example, the Identity Theft Resource Center reported 1,473
18 data breaches in 2019, which represents a 17 percent increase from the total number of
19 breaches reported in 2018. See Identity Theft Center, *2019 End-of-Year Data Breach*
20 *Report*, available at [https://www.idtheftcenter.org/wp-](https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf)
21 [content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-](https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf)
22 [Report_FINAL_Highres-Appendix.pdf](https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf).

23 33. It is not surprising that hotels have been frequent targets for hackers. As noted
24 by one cybersecurity expert, “hotels are an attractive target for hackers because they hold
25 a lot of sensitive information, including credit card and passport details, but often don’t
26 have security standards as tough as those of more regulated industries, like banking.”
27 Democrat-Gazette Staff Wire Reports, *Breach Puts Hotel Guests’ Data at Risk*,
28 ARKANSAS DEMOCRAT GAZETTE (Dec. 1, 2018),

1 <https://www.arkansasonline.com/news/2018/dec/01/breach-puts-hotel-guests-data-at-risk-2/>

2 34. The Personal Information of the type exposed in the data breach here remains
3 of high value to identity criminals, as evidenced by the prices criminals will pay through
4 black-market sources on the dark web. Numerous sources cite dark web pricing for stolen
5 identity credentials, quantifying the loss to victims based on the value of the data itself.
6 *Here's How Much Thieves Make By Selling Your Personal Data Online*, BUSINESS
7 INSIDER (May 27, 2015), available at [http://www.businessinsider.com/heres-how-much-](http://www.businessinsider.com/heres-how-much-your-personal-data-costs-on-the-dark-web-2015-5)
8 [your-personal-data-costs-on-the-dark-web-2015-5](http://www.businessinsider.com/heres-how-much-your-personal-data-costs-on-the-dark-web-2015-5).

9 35. Annual monetary losses for victims of identity theft are in the billions of
10 dollars. In 2017 alone, fraudsters stole \$16.8 billion from consumers in the United States,
11 which includes \$5.1 billion stolen through bank account take-overs. Javelin, *2018 Identity*
12 *fraud: Fraud Enters A New Era of Complexity*, available at
13 [https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-](https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity)
14 [era-complexity](https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity).

15 36. The annual cost of identity theft is even higher. McAfee and the Center for
16 Strategic and International Studies estimates that the likely annual cost to the global
17 economy from cybercrime is \$445 billion a year. Insurance Information Institute, *Facts +*
18 *Statistics: Identity theft and cybercrime*, available at [https://www.iii.org/fact-statistic/facts-](https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime)
19 [statistics-identity-theft-and-cybercrime](https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime).

20 37. Reimbursing a consumer for a financial loss due to fraud does not make that
21 individual whole again. On the contrary, in addition to the irreparable damage that may
22 result from the theft of personal information, identity theft victims must spend numerous
23 hours and their own money repairing the impact to their credit. After conducting a study,
24 the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft
25 victims "reported spending an average of about 7 hours clearing up the issues" and
26 resolving the consequences of fraud in 2014. U.S. Department of Justice, *Victims of*
27 *Identity Theft, 2014* (Revised November 13, 2017), available at
28 <http://www.bjs.gov/content/pub/pdf/vit14.pdf>.

1 38. The impact of identity theft can have ripple effects, which can adversely affect
2 the future financial trajectories of victims' lives. For example, the Identity Theft Resource
3 Center reports that respondents to their surveys in 2013-2016 described that the identity
4 theft they experienced affected their ability to get credit cards and obtain loans, such as
5 student loans or mortgages. Identity Theft Resource Center, *Identity Theft: The Aftermath*
6 *2017*, available at https://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf.

7 39. Evidence shows identity theft exacts a severe emotional toll on its victims.
8 The 2017 Identity Theft Resource Center survey evidences the emotional suffering
9 experienced by victims of identity theft:

- 10 • 75% of respondents reported feeling severely distressed
- 11 • 67% reported anxiety
- 12 • 66% reported feelings of fear related to personal financial safety
- 13 • 37% reported fearing for the financial safety of family members
- 14 • 24% reported fear for their physical safety
- 15 • 15.2% reported a relationship ended or was severely and negatively
- 16 impacted by the identity theft
- 17 • 7% reported feeling suicidal.

18 40. Identity theft can also exact a physical toll on its victims. The same survey
19 reported that respondents experienced physical symptoms stemming from their experience
20 with identity theft:

- 21 • 48.3% of respondents reported sleep disturbances
- 22 • 37.1% reported an inability to concentrate / lack of focus
- 23 • 28.7% reported they were unable to go to work because of physical
- 24 symptoms
- 25 • 23.1% reported new physical illnesses (aches and pains, heart
- 26 palpitations, sweating, stomach issues)
- 27 • 12.6% reported a start or relapse into unhealthy or addictive behaviors.

28 41. There may also be a significant time lag between when personal information

1 is stolen and when it is actually misused. According to the U.S. Government
2 Accountability Office (“GAO”), which conducted a study regarding data breaches:

3 [L]aw enforcement officials told us that in some cases, stolen
4 data may be held for up to a year or more before being used to
5 commit identity theft. Further, once stolen data have been sold
6 or posted on the Web, fraudulent use of that information may
7 continue for years. As a result, studies that attempt to measure
8 the harm resulting from data breaches cannot necessarily rule out
9 all future harm. U.S. Government Accountability Office, *Report*
10 *to Congressional Requesters* (June 2007),
11 <http://www.gao.gov/new.items/d07737.pdf>

12 42. Plaintiffs and the Class (as defined below) would not have provided their
13 account information and other Personal Information to Marriott if they had known Marriott
14 did not have in place adequate policies and procedures to protect their Personal
15 Information.

16 43. As the result of Marriott’s data breach, Plaintiff and class members have
17 suffered or will suffer economic loss and other actual harm for which they are entitled to
18 damages, including, but not limited to, the following:

- 19 • Potentially having to purchase services they would not have otherwise
20 paid for and/or paying more for services than they otherwise would
21 have paid, had they known the truth about Marriott’s substandard data
22 security practices;
- 23 • losing the inherent value of their Personal Information;
- 24 • identity theft and fraud resulting from theft of their Personal
25 Information;
- 26 • costs associated with the detection and prevention of identity theft and
27 unauthorized use of their online accounts;
- 28 • lowered credit scores resulting from credit inquiries following
fraudulent activities;
- costs associated with time spent and the loss of productivity or
enjoyment of one’s life from taking time to address and attempt to
mitigate and address the actual and future consequences of the Marriott
data breach, including discovering fraudulent charges, cancelling and

1 reissuing cards, imposing withdrawal and purchase limits on
2 compromised accounts, and the stress, nuisance, and annoyance of
dealing with the repercussions of the data breach; and

- 3 • the continued imminent and certainly impending injury flowing from
4 potential fraud and identity theft posed by their Personal Information
5 being in the possession of one or more unauthorized third parties.

6 44. Additionally, Plaintiff and class members place significant value in data
7 security. According to a recent survey conducted by cyber-security company FireEye,
8 approximately 50% of consumers consider data security to be a main or important
9 consideration when making purchasing decisions and nearly the same percentage would
10 be willing to pay more in order to work with a provider that has better data security.
11 Likewise, 70% of consumers would provide less personal information to organizations
12 that suffered a data breach. FireEye, *Beyond the Bottom Line: The Real Cost of Data*
13 *Breaches* (May 11, 2016), [https://www.fireeye.com/blog/executive-](https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html)
14 [perspective/2016/05/beyond_the_bottomli.html](https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html).

15 45. Accordingly, had consumers known the truth about Marriott's data security
16 practices—that Marriott would not adequately protect and store their data—they would not
17 have entrusted their Personal Information to Marriott, created a Marriott Bonvoy account,
18 and would not have been willing to pay for, or pay as much for, hotel stays at Marriott. As
19 such, Plaintiff and class members did not receive the benefit of their bargain with Marriott
20 because they paid for a value of services, either through Personal Information or a
21 combination of their Personal Information and money, they expected but did not receive.

22 V. CLASS ACTION ALLEGATIONS

23 46. Plaintiff brings this action on behalf of himself and all persons similarly
24 situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil
25 Procedure and seeks certification of the following class:

26 All persons in the State of California whose Personal
27 Information was stolen, disclosed, or accessed without
28 authorization in the data breach incident Marriott announced on

1 March 31, 2020.

2 47. The above-described class of persons shall hereafter be referred to as the
3 “Class.” Excluded from the Class are Marriott’s officers, directors, legal representatives,
4 successors, subsidiaries, and assigns, and any judge who presides over this action.

5 48. Plaintiff reserves the right to expand, limit, modify, or amend the class
6 definitions stated above, including the addition of one or more subclasses, in connection
7 with his motion for class certification, or at any other time, based upon, among other things,
8 changing circumstances, or new facts obtained during discovery.

9 49. **Numerosity.** The Class is so numerous that joinder of all members in one
10 action is impracticable. The exact number and identities of the members of the Class is
11 unknown to Plaintiff at this time and can only be ascertained through appropriate discovery,
12 but on information and belief, Plaintiff alleges that there are in excess of 1 Million members
13 of the Class.

14 50. **Typicality.** Plaintiff’s claims are typical of those of other members of the
15 Class, all of whom have suffered similar harm due to Defendants’ course of conduct as
16 described herein.

17 51. **Adequacy of Representation.** Plaintiff is an adequate representative of the
18 Class and will fairly and adequately protect the interests of the Class. Plaintiff has retained
19 attorneys who are experienced in the handling of complex litigation and class actions, and
20 Plaintiff and his counsel intend to prosecute this action vigorously.

21 52. **Existence and Predominance of Common Questions of Law or Fact.**
22 Common questions of law and fact exist as to all members of the Class that predominate
23 over any questions affecting only individual members of the Class. These common legal
24 and factual questions, which do not vary among members of the Class, and which may be
25 determined without reference to the individual circumstances of any member of the Class,
26 include, but are not limited to, the following:

- 27 (a) Whether Marriott owed a duty to Plaintiff and the Class to implement
28 and maintain reasonable security procedures and practices to protect
their Personal Information;

- 1 (b) Whether Marriott violated its duty to implement and maintain
2 reasonable security procedures and practices appropriate to the nature
3 of the information to protect the Personal Information of Plaintiff and
4 members of the Class.
5 (c) Whether the Personal Information compromised in the data breach was
6 information that is protected by California law;
7 (d) Whether Marriott knew or should have known that its computer and
8 data storage systems were vulnerable to attack;
9 (e) Whether Marriott failed to take available steps to prevent and stop the
10 data breach from occurring;
11 (f) Whether Marriott's failure to secure Plaintiff's and the Class's Personal
12 Information in the manner alleged violated federal, state and local laws,
13 or industry standards;
14 (g) Whether Marriott's conduct, including its failure to act, resulted in or
15 was the proximate cause of the data breach, resulting in the
16 unauthorized access to and/or theft of Plaintiff's' and the Class's
17 Personal Information;
18 (h) Whether Marriott has a contractual obligation to use reasonable security
19 measures and whether it complied with such contractual obligation;
20 (i) Whether Marriott's conduct amounted to violations of California
21 consumer protection statutes, and/or California data breach statutes;
22 (j) Whether, as a result of Marriott's conduct, Plaintiff and members of the
23 Class face a significant threat of harm and/or have already suffered
24 harm, and, if so, the appropriate measure of damages to which they are
25 entitled;
26 (k) Whether, as a result of Marriott's conduct, Plaintiff and members of the
27 Class are entitled to injunctive, equitable, declaratory and/or other
28 relief, and, if so, the nature of such relief.

53. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of this controversy, because individual litigation of the claims of all members of the Class is impracticable. Requiring each individual class member to file an individual lawsuit would unreasonably consume the amounts that may be recovered. Even if every member of the Class could afford individual litigation, the adjudication of at least tens of thousands of identical claims would be unduly burdensome to the courts.

1 and valuable Personal Information on its computer and data storage systems.

2 57. By collecting, storing, using, and profiting from this data, Marriott had a duty
3 of care to Plaintiff and the Class to exercise reasonable care in obtaining, retaining,
4 securing, safeguarding, deleting, and protecting this Personal Information in Marriott's
5 possession from being compromised, lost, stolen, accessed, and misused by unauthorized
6 persons. More specifically, this duty included, among other things: (a) designing,
7 maintaining, and testing Marriott's security systems and data storage architecture to ensure
8 that Plaintiff and the Class's Personal Information was adequately secured and protected;
9 (b) implementing processes that would detect an unauthorized breach of Marriott's security
10 systems and data storage architecture in a timely manner; (c) timely acting on all warnings
11 and alerts, including public information, regarding Marriott's security vulnerabilities and
12 potential compromise of the compiled data of Plaintiff and the Class; (d) maintaining and
13 implementing data security measures consistent with industry standards; and (e) instituting
14 data security policies and procedures, and adequately training employees and franchisees
15 on such policies and procedures.

16 58. Marriott had common law duties to prevent foreseeable harm to Plaintiff and
17 the Class. These duties existed because Plaintiff and members of the Class were the
18 foreseeable and probable victims of any inadequate security practices. In fact, not only
19 was it foreseeable that Plaintiff and the Class would be harmed by the failure to protect
20 their Personal Information because hackers routinely attempt to steal such information and
21 use it for nefarious purposes, Marriott knew that it was more likely than not Plaintiff and
22 other class members would be harmed by such theft.

23 59. Marriott had a duty to monitor, supervise, control, or otherwise provide
24 oversight to safeguard the Personal Information that was collected and stored on Marriott's
25 computer systems.

26 60. Marriott's duties to use reasonable security measures also arose as a result of
27 the special relationship that existed between Marriott, on the one hand, and Plaintiff and
28 members of the Class, on the other hand. The special relationship arose because Plaintiff

1 and members of the Class entrusted Defendant with their Personal Information in order to
2 make and pay for reservations at Marriott properties and/or create user accounts necessary
3 to access the Marriott Bonvoy program. Marriott alone could have ensured that its security
4 systems and data storage architecture were sufficient to prevent or minimize the data
5 breach.

6 61. Marriott knew or should have known that its computer systems and data
7 storage architecture were vulnerable to unauthorized access and targeting by hackers for
8 the purpose of stealing and misusing confidential Personal Information.

9 62. Marriott breached the duties it owed to Plaintiff and class members described
10 above and thus were negligent. Marriott breached these duties by, among other things,
11 failing to: (a) exercise reasonable care and implement adequate security systems, protocols
12 and practices sufficient to protect the Personal Information of Plaintiff and the Class; (b)
13 detect the breach while it was ongoing; (c) maintain security systems consistent with
14 industry standards; and (d) institute data security policies and procedures, and adequately
15 train employees and franchisees on such policies and procedures.

16 63. But for Marriott's wrongful and negligent breach of its duties owed to Plaintiff
17 and the Class members, their Personal Information would not have been compromised.

18 64. As a direct and proximate result of Marriott's negligence, Plaintiff and the
19 Class have been injured and are entitled to damages in an amount to be proven at trial.
20 Such injuries include one or more of the following: ongoing, imminent, certainly
21 impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary
22 loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in
23 monetary loss and economic harm; loss of the value of their privacy and the confidentiality
24 of the stolen Personal Information; illegal sale of the compromised Personal Information
25 on the black market; mitigation expenses and time spent on credit monitoring, identity theft
26 insurance, and credit freezes and unfreezes; time spent in response to the data breach
27 reviewing bank statements, credit card statements, and credit reports; expenses and time
28 spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value

1 of the Personal Information; lost benefit of their bargains and overcharges for services; and
2 other economic and non-economic harm.

3
4 **COUNT TWO**

5 **VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT (CAL. CIV**
6 **CODE § 1798.100, *et seq.*)**

7 **(By Plaintiff Against Defendants on Behalf of the Class)**

8 65. Plaintiff restates and re-alleges paragraphs 1 through 64 as if fully set forth
9 herein.

10 66. The California Consumer Privacy Act (“CCPA”), portions of which were
11 operative beginning January 1, 2020, was enacted by the California Legislature “to further
12 the constitutional right of privacy and to supplement existing laws relating to consumers’
13 personal information, including, but not limited to, Chapter 22 (commencing with Section
14 22575) of Division 8 of the Business and Professions Code and Title 1.81 (commencing
15 with Section 1798.80).” Cal. Civ. Code § 1798.100. The CCPA applies to “the collection
16 and sale of all personal information collected by a business from consumers.” *Id.*

17 67. “Businesses,” defined to include a “corporation” that “collects consumers’
18 personal information” that “does business in the State of California” and has annual gross
19 revenues in excess of \$25 million, are required to comply with the CCPA. Cal. Civ. Code
20 § 1798.140(c). Marriott is a “business” under the CCPA.

21 68. The CCPA protect “consumers.” “Consumer” is defined as “a natural person
22 who is a California resident[.]” Cal. Civ. Code § 1798.140(g). Plaintiff and members of
23 the Class are “consumers” within the meaning of the CCPA.

24 69. The protections of the CCPA extend to “personal information” of consumers.
25 “Personal information” is defined by the CCPA to include “information that identifies,
26 relates to, describes, is reasonably capable of being associated with, or could reasonably be
27 linked, directly or indirectly, with a particular consumer or household.” Cal. Civ. Code §
28 1798.140(o)(1). “Personal information includes, but is not limited to, the following if it

1 identifies, relates to, describes, is reasonably capable of being associated with, or could be
2 reasonably linked, directly or indirectly, with a particular consumer or household: (A)
3 Identifiers such as a *real name*, alias, *postal address*, unique personal identifier, online
4 identifier, internet protocol address, *email address*, *account name*, social security number,
5 driver's license number, passport number, or other similar identifiers.” Cal. Civ. Code §
6 1798.140(o)(1)(A) (emphasis added). It may also include a “telephone number,” Cal. Civ.
7 Code § 1798.140(o)(1)(B), Cal. Civ. Code § 1798.80(e), as well as “[c]ommercial
8 information, including . . . products or services purchased, obtained, or considered, or other
9 purchasing or consuming histories or tendencies” and “[p]rofessional or employment-
10 related information.” Cal. Civ. Code § 1798.140(o)(1)(D) & (I). The Personal Information
11 of Plaintiff and members of the Class that was compromised in Marriott’s data breach
12 included “personal information” within the meaning of the CCPA.

13 70. The CCPA provides consumers with the right to institute a civil action where
14 the consumers’ “nonencrypted and nonredacted personal information” was the subject of
15 “an unauthorized access and exfiltration, theft, or disclosure as a result of the business’s
16 violation of the duty to implement and maintain reasonable security procedures and
17 practices appropriate to the nature of the information to protect the personal information .
18 . . .” Cal. Civ. Code § 1798.150(a)(1).

19 71. Marriott, as a “business” covered by the CCPA, owed a duty to Plaintiff and
20 members of the Class to implement and maintain reasonable security procedures and
21 practices” to protect the Personal Information of Plaintiff and members of the Class.

22 72. Marriott breached this duty. On March 31, 2020, Marriott announced a data
23 breach affecting 5.2 million customers, a large portion of whom are members of the Class.
24 Marriott admitted that at the end of February 2020, it “identified that an unexpected amount
25 of guest information may have been accessed using the login credentials of two employees
26 at a franchise property.” According to Marriott, “[w]e believe this activity started in mid-
27 January 2020.” Marriott also admitted that contact details (e.g., name, mailing address,
28 email address, and phone number), Loyalty Account Information (e.g., account number

1 and points balance), additional personal details (e.g., company, gender, and birthday day
2 and month), partnerships and affiliations (e.g., linked airline loyalty programs and
3 numbers), and preferences (e.g., stay/room preferences and language preference) may all
4 have been accessed in the breach.

5 73. With regard to Plaintiff, Marriott apologized to him and admitted that his
6 personal information was accessed without his authorization, including, his contact details
7 (e.g., name, mailing address, email address, and phone number), additional personal details
8 (e.g., company, gender, and birthday day and month), loyalty account information (e.g.,
9 account number and points balance), partnerships and affiliations (e.g., linked airline
10 loyalty programs and numbers), and preferences (e.g., stay/room preferences and language
11 preference).”

12 74. The fact that Plaintiff’s and the Class’s Personal Information was accessed
13 without authorization establishes that Marriott did not take adequate data security measures
14 to store and protect its guests’ Personal Information. Marriott failed to take adequate
15 security measures to protect Plaintiff’s and the class members’ Personal Information.

16 75. As a direct and proximate result of Marriott’s acts and omissions, Plaintiff
17 and the members of the Class were subjected to unauthorized access and exfiltration, theft,
18 or disclosure as a result of Defendants’ violation of the duty.

19 76. On behalf of the Class, Plaintiff seeks injunctive relief in the form of an order
20 (a) enjoining Marriott from continuing to violate the CCPA, (b) requiring Marriott to
21 employ adequate security practices consistent with law and industry standards to protect
22 class members’ personal information, (c) requiring Marriott to complete its investigation,
23 and (d) issuing an amended statement to the public and affected guests that is not evasive
24 and contains no equivocations (e.g., phrases such as “may have,” the investigation is
25 “ongoing,” “no reason to believe,” etc.) and to instead confirm and confess, with certainty,
26 what categories of data were stolen and accessed without class members’ authorization,
27 how the data breach occurred, and what specifically occurred to cause the breach.

28 77. Plaintiff presently seeks only injunctive relief and any other relief the court

1 deems proper pursuant to this section, such as attorneys’ fees. Prior to initiating this action,
2 Plaintiff served written notice identifying Marriott’s violations of section 1798.150(a) and
3 demanding that the data breach be cured. If within 30 days, Marriott has not cured, Plaintiff
4 will amend this Complaint to seek statutory damages pursuant to Civil Code section
5 1798.150(a)(1)(A).

6
7 **COUNT THREE**

8 **BREACH OF CONTRACT**

9 **(By Plaintiff Against Defendants on Behalf of the Class)**

10 78. Plaintiff restates and re-alleges paragraphs 1 through 77 as if fully set forth
11 herein.

12 79. Marriott’s Global Privacy Statement dated June 3, 2019 and its California
13 Privacy Statement dated January 1, 2020 (together, the “Privacy Policy”) is an agreement
14 between Marriott and persons who provide their Personal Information to Marriott,
15 including Plaintiff and the Class.

16 80. The Global Privacy Statement, as it was in effect at the time of the Marriott
17 data breach, applies to persons from whom Marriott has collected Personal Information.
18 When read together with the California Privacy Statement, the two documents apply to
19 California residents from whom Marriott has collected Personal Information.

20 81. The Privacy Policy provides detailed information about what types of
21 Personal Information will be shared, with what entities, and how it is collected. Marriott
22 assures customers, including Plaintiff and the Class, that “[t]he Marriott Group, which
23 includes Marriott International, Inc. . . . values you as our guest and recognizes that privacy
24 is important to you.” Marriott Group also assures customers, including Plaintiff and the
25 Class, that “[w]e seek to use reasonable organizational, technical and administrative
26 measures to protect Personal Data.” Further, Marriott delineates in the Privacy Policy the
27 universe of persons and entities who are authorized to receive Personal Information of
28 customers, including Plaintiff and the Class, and what specific categories of Personal

1 Information they are authorized to receive. Any disclosures of Personal Information that
2 deviate from the Privacy Policy are not authorized disclosures.

3 82. Plaintiff and members of the Class, on the one hand, and Marriott on the other
4 hand, formed a contract when Plaintiff and members of the Class members provided
5 Personal Information to Marriott subject to the Privacy Policy.

6 83. Plaintiff and the Class fully performed their obligations under the contract
7 with Marriott.

8 84. Marriott breached its agreement with Plaintiff and the Class by failing to
9 protect their Personal Information and permitting disclosures of Personal Information that
10 deviated from, and were inconsistent with, the Privacy Policy. Specifically, Marriott (1)
11 failed to use reasonable measures to protect that Personal Information; and (2) disclosed
12 that information to unauthorized third parties, in violation of the agreement.

13 85. As a direct and proximate result of these breaches of contract, Plaintiff and
14 the Class sustained actual losses and damages as described in detail above, including but
15 not limited to, that they did not get the benefit of the bargain pursuant to which they
16 provided their Personal Information to Marriott.

17
18 **COUNT FOUR**

19 **BREACH OF IMPLIED CONTRACT**

20 **(By Plaintiff Against Defendants on Behalf of the Class)**

21 86. Plaintiff restates and re-alleges paragraphs 1 through 85 as if fully set forth
22 herein.

23 87. Plaintiff and the Class also entered into an implied contract with Marriott
24 when they obtained services from Marriott, or otherwise provided Personal Information to
25 Marriott.

26 88. As part of these transactions, Marriott agreed to safeguard and protect the
27 Personal Information of Plaintiff and the Class.

28 89. Plaintiff and members of the Class entered into implied contracts with the

1 reasonable expectation that Marriott's data security practices and policies were reasonable
2 and consistent with industry standards. Plaintiff and the Class believed that Marriott would
3 use part of the monies paid to Marriott, or monies which it derived from sharing the
4 Personal Information with third parties, under the implied contracts to fund adequate and
5 reasonable data security practices.

6 90. Plaintiff and the Class would not have provided and entrusted their Personal
7 Information to Marriott or would have paid less for Marriott's services in the absence of
8 the implied contract or implied terms between them and Marriott. The safeguarding of the
9 Personal Information of Plaintiffs and class members was critical to realize the intent of
10 the parties.

11 91. Plaintiff and the Class fully performed their obligations under the implied
12 contracts with Marriott.

13 92. Marriott breached its implied contracts with Plaintiff and the Class to protect
14 their Personal Information when it (1) failed to have security protocols and measures in
15 place to protect that information; and (2) disclosed that information to unauthorized third
16 parties.

17 93. As a direct and proximate result of these breaches of implied contract, Plaintiff
18 and the Class sustained actual losses and damages as described in detail above, including
19 but not limited to, that they did not get the benefit of the bargain pursuant to which they
20 provided their Personal Information to Marriott.

21
22 **COUNT FIVE**

23 **VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW (CAL.**
24 **BUS. & PROF. CODE § 17200, *et seq.*)**

25 **(By Plaintiff Against Defendants on Behalf of the Class)**

26 94. Plaintiff restates and re-alleges paragraphs 1 through 93 as if fully set forth
27 herein.

28 95. California Business and Professions Code section 17200 *et seq.*, also known

1 as the California Unfair Competition Law (“UCL”), prohibits acts of “unfair competition,”
2 including any “unlawful, unfair or fraudulent business act or practice.”

3 96. A cause of action may be brought under the “unlawful” prong of the UCL if
4 a practice violates another law. Such an action borrows violations of other laws and treats
5 these violations, when committed pursuant to business activity, as unlawful practices
6 independently actionable under the UCL.

7 97. Here, Marriott’s “unlawful” acts and practices include violating California
8 Civil Code section 1798.150 as described above, and failing to implement and maintain
9 reasonable security measures contrary to legislatively declared public policy that seeks to
10 protect consumers’ data and ensure that entities that are trusted with it use appropriate
11 security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C.
12 § 45 and California’s Consumer Records Act, Cal. Civ. Code § 1798.81.5.

13 98. A business act or practice is “unfair” under the UCL if it offends an
14 established public policy or is immoral, unethical, oppressive, unscrupulous or
15 substantially injurious to consumers, and that unfairness is determined by weighing the
16 reasons, justifications and motives of the practice against the gravity of the harm to the
17 alleged victims.

18 99. Here, Marriott’s “unfair” acts and practices include:

19 (a) failing to abide by the provisions of California Civil Code section
20 1798.150

21 (b) failing to implement and maintain reasonable security measures
22 contrary to legislatively declared public policy that seeks to protect consumers’ data and
23 ensure that entities that are trusted with it use appropriate security measures. These policies
24 are reflected in laws, including the FTC Act, 15 U.S.C. § 45 and California’s Consumer
25 Records Act, Cal. Civ. Code § 1798.81.5.

26 (c) failing to implement and maintain reasonable security measures to
27 protect Plaintiff’s and the Class’s Personal Information from unauthorized disclosure,
28 release, data breaches, and theft, which was a direct and proximate cause of the data breach.

1 Marriott failed to identify foreseeable security risks, remediate identified security risks,
2 and adequately improve security despite knowing the risk of cybersecurity incidents. This
3 conduct, with little if any utility, is unfair when weighed against the harm to Plaintiff and
4 the Class, whose Personal Information has been compromised; and

5 (d) failing to implement and maintain reasonable security measures, which
6 also led to substantial consumer injuries, as described above, and which are not outweighed
7 by any countervailing benefits to consumers or competition. Moreover, because consumers
8 could not know of Marriott's inadequate security, consumers could not have reasonably
9 avoided the harms that Marriott caused.

10 100. A business act or practice is "fraudulent" within the meaning of the UCL if
11 members of the public are likely to be deceived.

12 101. Here, Marriott's "fraudulent" acts and practices include:

13 (a) misrepresenting that it would protect the privacy and confidentiality of
14 Plaintiff's and the Class's Personal Information, including by implementing and
15 maintaining reasonable security measures;

16 (b) Omitting, suppressing, and concealing the material fact that it did not
17 reasonably or adequately secure Plaintiff's and the Class's Personal Information; and

18 (c) Omitting, suppressing, and concealing the material fact that it did not
19 comply with common law and statutory duties pertaining to the security and privacy of
20 Plaintiff's and the Class's Personal Information, including duties imposed by the CCPA
21 and the FTC Act.

22 102. Marriott's representations and omissions were material because they were
23 likely to deceive reasonable consumers about the adequacy of Marriott's data security and
24 ability to protect the confidentiality of consumers' Personal Information.

25 103. As a direct and proximate result of Marriott's unfair, unlawful, and fraudulent
26 acts and practices, Plaintiff and the Class were injured and lost money or property,
27 including, but not limited to: the money received by the Marriott for its services; the loss
28 of the benefit of their bargain with and overcharges by Marriott as they would not have

1 paid Marriott for services or would have paid less for such services but for the violations
2 alleged herein; losses from fraud and identity theft; any costs they will have to incur for
3 credit monitoring and identity protection services; time and expenses related to monitoring
4 their financial accounts for fraudulent activity; loss of value of their Personal Information;
5 and an increased, imminent risk of fraud and identity theft.

6 104. Plaintiff and the Class seek all monetary and non-monetary relief allowed by
7 law, including restitution of all profits stemming from Marriott's unfair, unlawful, and
8 fraudulent business practices or use of their Personal Information; declaratory relief;
9 reasonable attorneys' fees and costs under California Code of Civil Procedure section
10 1021.5; injunctive relief; and other appropriate equitable relief.

11
12 **COUNT SIX**

13 **UNJUST ENRICHMENT**

14 **(By Plaintiff Against Defendants on Behalf of the Class, or in the Alternative, the**
15 **California Class)**

16 105. Plaintiff restates and re-alleges paragraphs 1 through 104 as if fully set forth
17 herein.

18 106. Plaintiff and the Class have an interest, both equitable and legal, in the
19 Personal Information about them that was furnished to, collected by, and maintained by
20 Marriott and that was ultimately stolen in the data breach.

21 107. Marriott was benefited by the conferral upon it of the Personal Information
22 pertaining to Plaintiff and the Class and by its ability to retain, use, and profit from that
23 information. Marriott understood that it was in fact so benefited.

24 108. Marriott also understood and appreciated that the Personal Information
25 pertaining to Plaintiff and the Class was private and confidential and its value depended
26 upon Marriott maintaining the privacy and confidentiality of that Personal Information.

27 109. But for Marriott's willingness and commitment to maintain its privacy and
28 confidentiality, that Personal Information would not have been transferred to and entrusted

1 with Marriott.

2 110. Marriott continues to benefit and profit from its retention and use of the
3 Personal Information while its value to Plaintiff and the Class has been diminished.

4 111. Marriott also benefitted through its unjust conduct by retaining money that it
5 should have used to provide reasonable and adequate data security to protect Plaintiff and
6 the Class's Personal Information.

7 112. It is inequitable for Marriott to retain these benefits.

8 113. As a result of Marriott's wrongful conduct as alleged in this Complaint
9 (including, among other conduct, its knowing failure to employ adequate data security
10 measures, its continued maintenance and use of the Personal Information belonging to
11 Plaintiff and class members without having adequate data security measures, and its other
12 conduct facilitating the theft of that Personal Information), Marriott has been unjustly
13 enriched at the expense of, and to the detriment of, Plaintiff and the Class.

14 114. Marriott's unjust enrichment is traceable to, and resulted directly and
15 proximately from, the conduct alleged herein, including the compiling and use of Plaintiff
16 and class members' Personal Information, while at the same time failing to maintain that
17 information secure from intrusion and theft by hackers and identity thieves.

18 115. Under the common law doctrine of unjust enrichment, it is inequitable for
19 Marriott to be permitted to retain the benefits it received, and is still receiving, without
20 justification, from Plaintiff and the Class in an unfair and unconscionable manner.
21 Marriott's retention of such benefits under circumstances making it inequitable to do so
22 constitutes unjust enrichment.

23 116. The benefits conferred upon, received, and enjoyed by Marriott were not
24 conferred officiously or gratuitously, and it would be inequitable and unjust for Marriott to
25 retain these benefits.

26 117. Plaintiff and the Class have no adequate remedy at law.

27 118. Marriott is therefore liable to Plaintiff and the Class for restitution or
28 disgorgement in the amount of the benefit conferred on Marriott as a result of its wrongful

1 conduct, including specifically: the value to Marriott of the Personal Information that was
2 stolen in the data breach; the profits Marriott is receiving from the use of that information;
3 and the amounts that Marriott should have spent to provide reasonable and adequate data
4 security to protect Plaintiffs' and class members' Personal Information.

5
6 **VII. PRAYER FOR RELIEF**

7 WHEREFORE, Plaintiff, individually and on behalf of all members of the Class,
8 prays for judgment against Defendants, and each of them, as follows:

9 1. For an order certifying that the action be maintained as a class action under
10 Rule 23(b)(2), Rule 23(b)(3), and/or 23(c)(4) of the Federal Rules of Civil Procedure, that
11 Plaintiff be designated the class representative, and that undersigned counsel be designated
12 as class counsel.

13 2. For injunctive and other equitable relief as is necessary to protect the interests
14 of Plaintiff and members of the Class, including but not limited to an order:

15 (a) Prohibiting Marriott from engaging in the wrongful and unlawful acts
16 described herein;

17 (b) Requiring Marriott to protect, including through adequate encryption,
18 all data collected through the course of its business in accordance with all applicable
19 regulations, industry standards, and federal, state, or local laws;

20 (c) Requiring Marriott to implement and maintain a comprehensive
21 Information Security Program designed to protect the confidentiality and integrity of
22 Plaintiff's and class members' Personal Information;

23 (d) Requiring Marriott to engage independent third-party security auditors
24 and internal personnel to run automated security monitoring;

25 (e) Requiring Marriott to audit, test, and train its security personnel
26 regarding any new or modified procedures;

27 (f) Requiring Marriott to segment data by, among other things, creating
28 firewalls and access controls so that if one area of Marriott's network is compromised,

1 hackers cannot gain access to other portions of Marriott's systems;

2 (g) Requiring Marriott to conduct regular database scanning and security
3 checks;

4 (h) Requiring Marriott to establish an information security training
5 program that includes at least annual information security training for all employees, with
6 additional training to be provided as appropriate based upon employees' respective
7 responsibilities with handling Personal Information, as well as protecting the Personal
8 Information of Plaintiff and the Class;

9 (i) Requiring Marriott to routinely and continually conduct internal
10 training and education, at least annually, to inform security personnel how to identify and
11 contain a breach when it occurs and what to do in response to a breach;

12 (j) Requiring Marriott to implement, maintain, regularly review, and revise
13 as necessary, a threat management program designed to appropriately monitor the
14 Marriott's information networks for threats, both internal and external, and assess whether
15 monitoring tools are appropriately configured, tested, and updated;

16 (k) Requiring Marriott to meaningfully educate all class members about the
17 threats they face as a result of the loss of their Personal Information to third parties, as well
18 as the steps affected individuals must take to protect themselves; and

19 (l) Requiring Marriott to implement logging and monitoring programs
20 sufficient to track traffic to and from Marriott's servers.

21 3. For an award of compensatory, consequential, and general damages, including
22 nominal damages, as allowed by law in an amount to be determined at trial;

23 4. For an award of restitution or disgorgement, in an amount to be determined at
24 trial;

25 5. For an award of attorneys' fees, costs, and litigation expenses pursuant to
26 California Code of Civil Procedure section 1021.5 or as otherwise allowed by law;

27 6. For prejudgment interest on all amounts awarded; and

28 7. For such other and further relief as the Court may deem just and proper.

1 Dated: April 3, 2020

AI LAW, PLC

2
3 By: /s/ Ahmed Ibrahim
4 Ahmed Ibrahim
5 Attorneys for Plaintiff, Individually and
6 On Behalf of All Others Similarly Situated

7 **JURY DEMAND**

8 Plaintiff, on behalf of himself and all others similarly situated, hereby demands a
9 trial by jury on all issues so triable.
10

11 Dated: April 3, 2020

AI LAW, PLC

12
13 By: /s/ Ahmed Ibrahim
14 Ahmed Ibrahim
15 Attorneys for Plaintiff, Individually and
16 On Behalf of All Others Similarly Situated
17
18
19
20
21
22
23
24
25
26
27
28